

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

The residence located at 3344 Thunderbird Court, Columbus
OH 43228 and any person, computers and/or digital media
located therein

Case No.

2:17-mj-710

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT B, INCORPORATED HEREIN BY REFERENCE

located in the Southern District of Ohio, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT A, INCORPORATED HEREIN BY REFERENCE

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

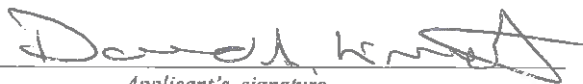
Code Section
18 U.S.C. Sec 2252 and
2252A

Offense Description
Receipt, distribution and/or possession of child pornography or visual depictions of minors engaged in sexually explicit conduct via a means or facility of interstate commerce

The application is based on these facts:

SEE ATTACHED AFFIDAVIT INCORPORATED HEREIN BY REFERENCE

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

David A. Knight, SA FBI

Printed name and title

Sworn to before me and signed in my presence.

Date:

11/27/17



Judge's signature

City and state: Columbus, Ohio

Kimberly A. Jolson, U.S. Magistrate Judge

Printed name and title

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT, EASTERN DIVISION OF OHIO**

In the Matter of the Search of:

)
)
)
)
)
)
)

No

2:17-mj-710

Magistrate Judge

**The residence located at
3344 Thunderbird Court
Columbus, Ohio 43228 and any person,
computers and/or digital media located
therein**

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, David A. Knight, a Special Agent with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION TRAINING AND EXPERIENCE

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Cincinnati Division and I have been a Special Agent since August 2007. I am currently assigned to the FBI Child Exploitation Task Force, investigating matters involving the online exploitation of children and child pornography. Prior to joining the FBI, I was a Columbus, Ohio Police Officer for 8 years, also working on the FBI Child Exploitation Task Force. I have made arrests and have executed search warrants pertaining to these types of investigations.

2. During my career as a police officer and Special Agent, I have participated in various investigations involving computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, digital media, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a Special Agent, I investigate criminal child exploitation and child pornography violations, including the illegal distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2252(a) and 2252A.

3. As a Special Agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

II. PURPOSE OF THE AFFIDAVIT

4. The facts set forth below are based upon my own personal observations, investigative reports, and information provided to me by other law enforcement agents. I have not included in this affidavit all information known by me relating to the investigation. I have set forth only the facts believed to be necessary to establish probable cause for a search warrant for the residential property located at 3344 Thunderbird Court, Columbus, Ohio 43228 (hereinafter, the “SUBJECT PREMISES”). I have not withheld any evidence or information that would negate probable cause.

5. The SUBJECT PREMISES to be searched is more particularly described in Attachment B, for the items specified in Attachment A, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2252 and 2252A B the receipt, and/or possession of child pornography. I am requesting authority to search the entire SUBJECT PREMISES, including the residential dwelling, all outbuildings, any person located therein who may be in possession of a mobile computing device, and any computer and computer-related media located therein where the items specified in Attachment A may be found, and to seize all items listed in Attachment A as instrumentalities, fruits, and evidence of crime.

III. APPLICABLE STATUTES AND DEFINITIONS

6. Title 18 United States Code, Section 2252 makes it a crime to knowingly transport, ship, receive, distribute, sell or possess in interstate commerce any visual depiction involving the use of a minor engaging in sexually explicit conduct.

7. Title 18 United States Code § 2252A makes it a crime to knowingly receive, distribute, possess, or access with intent to view any child pornography that has been mailed, or using any means or facility of interstate commerce.

8. As it is used in 18 U.S.C. §§ 2251 and 2252, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2)(A) as:

actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

9. As it is used in 18 U.S.C. § 2252A(a)(2), the term “child pornography” is defined in 18 U.S.C. § 2256(8) as: ¹

¹ The term child pornography is used throughout this affidavit. All subsequent references to this term in this affidavit

any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

10. The term “sexually explicit conduct” has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), “sexually explicit conduct” also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated; (i) bestiality; (ii) masturbation; (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

11. “Graphic” when used with respect to a depiction of sexually explicit conduct, means that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted. (18 U.S.C. § 2256(10))

12. The following terms have the same meanings or explanations in both statutes:

- A. “minor” means any person under the age of eighteen years (18 U.S.C. § 2256(1));
- B. “visual depiction” includes undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format (18 U.S.C. § 2256(5));
- C. “computer” is defined as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly

and all Attachments include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. § 2252 and child pornography as defined in 18 U.S.C. § 2256(8).

related to or operating in conjunction with such device. . .”(18 U.S.C. §§ 1030(e)(1) and 2256(6)).²

IV. BACKGROUND REGARDING COMPUTERS, MOBILE DEVICES AND THE INTERNET

13. Based on my knowledge, training, and experience, and the experience of other law enforcement officers, I have knowledge of the Internet and how it operates. I know that the Internet is a collection of computers and computer networks that are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information. Connections between Internet computers exist across state and international borders; therefore, information sent between two computers connected to the Internet frequently cross state and international borders even when the two computers are located in the same state. The following paragraphs describe some of the functions and features of the Internet as it relates to the subject of this search warrant.

14. A website is a collection of Internet pages that Internet users can view. The web address is the name given to a website that enables Internet users to find the website. When a user types in the web address while connected to the Internet, the user will be connected to that website.

15. Computers are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or camera-bearing smartphone, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including AGIF@ (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

16. Computers are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures

² The term "computer" is used throughout this affidavit to refer not only to traditional laptop and desktop computers, but also internet-capable devices such as cellular phones and tablets. Where the capabilities of these devices differ from that of a traditional computer, they are discussed separately and distinctly.

Experts Group) files.

17. A computer's capability to store images in digital form makes it an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as a hard drive) used in computers has grown tremendously within the last several years. Hard drives with the capacity of multiple terabytes are not uncommon. These drives can store tens of thousands of images at very high resolution. Other media storage devices include CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a USB (Universal Serial Bus) port on the computer. It is extremely easy for an individual to take or receive a photo or video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it to any one of those storage devices (CDs and DVDs are unique in that special software must be used to save or "burn" files to them).

18. Tablet devices have average storage capabilities ranging from 4 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person.

19. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography.

20. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties,

your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment A.

21. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily- available forensic tools. When a person "deletes" a file from a computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

22. Searches and seizures of evidence from computers and mobile computing devices commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored; and
- b. Searching computer systems for criminal evidence is a highly technical process

requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

23. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child pornography where the evidence consists partly of graphics files, any monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

24. In addition, there is probable cause to believe that any computer and its storage devices, monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2252 and 2252A, and should all be seized as such.

VI. SEARCH METHODOLOGY TO BE EMPLOYED

25. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in Attachment A;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment A;
- c. surveying various files, directories and the individual files they contain;
- d. opening files in order to determine their contents;
- e. scanning storage areas;

- f. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or
- g. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment A.

VII. INVESTIGATION AND PROBABLE CAUSE

26. On October 17, 2017, an employee arrived to work at the United Dairy Farmer's (hereinafter UDF) at 1188 N. Wilson Road, Columbus, Ohio at approximately 5:00 PM. The employee observed a black Samsung tablet sitting in the café area of the UDF. Assuming someone had forgotten the tablet, the employee secured it and place it in the office of the UDF. That evening no one returned to claim the tablet.

27. The next day, another employee arrived to work at the UDF and noticed the tablet in the office. The first employee, who was also at work at UDF that day, explained that someone had left the tablet in the store, and she was hoping they would return for it. Both employees then decided to look at the tablet to see if they could locate any owner information since no one had shown up to claim it. The tablet was not password protected and once opened the second employee clicked on the "Gallery" icon. Both employees immediately observed what they believed to be images of young children engaged in sex acts with adults and other children. The first employee called the Columbus Police Department to report what they had discovered and requested an officer come to their location.

28. Columbus Police Officer Colleen Theil was dispatched to the UDF in response to the all from the UDF employee. The first employee showed Officer Theil the tablet and stated they had only looked at it in order to try and find the owner. The second employee then clicked on the "Gallery" icon again and showed Officer Theil the images that they had seen previously when they accessed the "Gallery" folder. Officer Theil observed images of young children engaged in sexually explicit activity and believed the images to be child pornography.

29. Upon seeing the images, Officer Theil called the Columbus Police Exploited Children's Unit and reported what she had seen. Officer Theil was instructed to shut down the tablet and take it into evidence, which she did.

30. After Officer Theil left the UDF, an unknown male entered the store and asked one of the employees if anyone had turned in a tablet. The unknown male stated, "I may have left a tablet and folder over here", and pointed to the cafe area in the UDF. The UDF employee told the

unknown male that they had not found a tablet and nothing had been turned into the store. When the unknown male left the store, the UDF employee observed the unknown male get into a Grey Volvo S60 with an Ohio license plate # GLX1812.

31. The UDF employee then called the Columbus Police Department again and asked for an officer to respond to the UDF. At approximately 6:10 PM that evening, Officer Cain responded to the UDF and spoke with the employee. The employee explained the situation to Officer Cain and stated that he believed the unknown male was the owner of the tablet.

32. Officer Cain ran Ohio license plate # GLX1812 through NCIC/LEADS. The vehicle was registered to Cathy and Maxwell Godfrey. Officer Cain compared the UDF surveillance video to the driver's license photo of Maxwell Godfrey. They appeared to be the same individual. Furthermore, when Officer Cain ran Maxwell Godfrey through NCIC/LEADS it was discovered that Maxwell Godfrey is a registered sex offender in Franklin County, Ohio.

33. The tablet that was obtained from the UDF was subsequently identified as a Samsung Galaxy Tablet model SM-T820. The Samsung tablet was briefly analyzed by Detective Dave Blubaugh of the Columbus Police Exploited Children's Unit, who observed numerous child pornography images on the device. Detective Blubaugh thereafter contacted your affiant to determine whether federal charges would be pursued.

34. Your affiant subsequently ran Ohio license plate # GLX1812 through the Ohio Law Enforcement Gateway (OHLEG) database. The vehicle has a current registration address of the SUBJECT PREMISES. Additionally, your affiant conducted a search for Maxwell Godfrey in the Franklin County Sex Offender database. The sex offender database shows Maxwell Godfrey's current address at the SUBJECT PREMISES. Maxwell Godfrey was convicted on October 4th, 2013 of violating Ohio Revised Code 2907.322, Pandering Sexually Oriented Matter Involving a Minor.

35. On November 1, 2017, your affiant met with Detective Blubaugh and obtained the Samsung tablet. The following day, your affiant obtained a Federal Search warrant issued in the United States District Court for the Southern District of Ohio for the tablet.

36. On November 6, 2017, FBI Task Force Officer Brett Peachey completed a forensic examination of a 128 GB MicroSD card that was located in the Samsung tablet. The forensic examination revealed more than 20,000 images of child pornography located on the MicroSD card. Additionally, the forensic examination revealed more than 1,000 videos of child pornography located on the MicroSD card.

37. Further examination of the MicroSD card revealed that the images and videos of child pornography were categorized and stored in hundreds of folders that were labeled to detail exactly what was contained in each folder. The folder designations contained known titles of child pornography, which included children's ages and names. Examination of creation dates of the folders revealed that more than half of all the files on the MicroSD card were copied onto the card from a different device on April 18, 2017. From your affiant's training and experience it is more likely than not that, due to the large number of files that were copied on a single day and the size and organization of the folder structure, the files were originally stored on another device and copied to the Samsung tablet.

38. On November 6, 2017, your affiant completed a File System and Logical extraction examination of the Samsung tablet using Cellebrite 4PC software. Your affiant located several hundred cached images of child pornography on the tablet. Additionally, the email address maxgodfrey2000@gmail.com was associated with the user of the tablet.

39. The File System extraction of the Samsung tablet also revealed the wireless networks that the tablet had previously connected to in order to access the Internet. The extraction listed the Service Set Identifier (SSID) of each wireless network. An SSID is a name or identifier that is displayed by a wireless network so a potential user can identify it and access it to connect to the Internet. The extraction listed 17 SSIDs that the tablet had used previously. One of the SSID's listed had a name of 2WIRE989.

40. On November 8, 2017 Detective Dave Blubaugh parked in front of the SUBJECT PREMISES. Detective Blubaugh opened his wireless connection on his cellular phone and observed the available wireless networks in the area. The strongest wireless network signal appeared to be coming from the SUBJECT PREMISES and had an SSID of 2WIRE989.

41. On November 8, 2017, your affiant sent an administrative subpoena to AT&T Internet services for any customer information relating to the SUBJECT PREMISES. On November 18, 2017, AT&T Internet Services responded with the following information about Internet service at the SUBJECT PREMISES:

Account ID:	127406533
Account Name:	Cathy Godfrey
Service Address:	3344 Thunderbird CT
	Columbus, Ohio 43228
Preferred Email:	<u>maxgodfrey2000@gmail.com</u>

42. In summary, evidence discovered during the investigation in this matter indicates that the

Samsung tablet that was found at the UDF on October 17, 2017, belongs to Maxwell Godfrey. Godfrey is linked to the SUBJECT PREMISES by the registration of the vehicle he was observed driving when he went to the UDF on October 18, 2017, and inquired about the tablet, and through his sex offender registration. Godfrey is further linked to the Samsung tablet through the forensic examination, which revealed a user email address of maxgodfrey2000@gmail.com, as well as several thousand images of child pornography. The folder structure and creation dates of the child pornography files indicate that those files were not downloaded from the internet via the tablet, but were copied to the tablet from another device. Investigation of the SUBJECT PREMISES and information from the forensic examination of the tablet indicates that Godfrey has used a secured wireless network in the SUBJECT PREMISES to access the internet. Your affiant submits that all of the foregoing provides probable cause that Godfrey utilized an internet-capable device to access the internet at the SUBJECT PREMISES to download child pornography that was later transferred to the Samsung tablet.

VIII. CHILD PORNOGRAPHY COLLECTOR CHARACTERISTICS

39. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

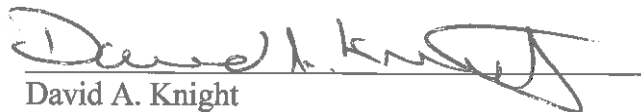
- A. Those who receive and may be collecting child pornography may obtain sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have while viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.
- B. Those who receive and may be collecting child pornography may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- C. Those who receive and may be collecting child pornography also may correspond with and/or meet others to share information and materials; rarely destroy

correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

- D. Those who receive and may be collecting child pornography prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography offenders throughout the world.
- E. When images and videos of child pornography are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years, even after such images and videos have been deleted from the computers or digital media.

IX. CONCLUSION

40. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that the SUBJECT PREMISES contains child pornography, that violations of Title 18, United States Code, Sections 2252 and 2252A have been committed, and evidence of those violations is located in the and evidence of those violations is located in the residence described in Attachment B, and on any computers or computer related media found therein. Your affiant, therefore, respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in Attachment A.



David A. Knight
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me this 27th day of November 2017.



Kimberly A. Jolson
United States Magistrate Judge
United States District Court, Southern District of Ohio

ATTACHMENT A
LIST OF ITEMS TO BE SEIZED

The terms "child pornography" and "visual depictions," as used herein, have the same definitions listed in Section III of the attached affidavit, and those definitions are incorporated herein by reference.

1. Computer(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, thumb or flash drives, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to an interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, P2P software.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography.
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography.
6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography.

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography.
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider, which could reveal information regarding the user(s) of the Internet Service at the SUBJECT PREMISES and what devices have accessed the Internet.
11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
12. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
13. Any and all cameras, film, videotapes or other photographic equipment.
14. Any and all visual depictions of minors, whether clothed or not, for comparison to and identification of any child pornography files that are discovered.

15. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, of any child pornography.
16. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described in Attachment B, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.
17. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.

**ATTACHMENT B
DESCRIPTION OF PLACE TO BE SEARCHED**

The SUBJECT PREMISES is a single-story ranch style brick residence with white siding, trim, and garage door. There is a covered front porch with a red front door with a white storm door. The numbers 3344 are located above the garage door.

The premises to be searched includes any persons located within the residence who may be carrying a mobile computing or digital storage device, and any appurtenances to the real property that is 3344 Thunderbird Court, Columbus, Ohio 43228, to include any storage units/outbuildings.

